IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Satoru TANAKA

Serial No. 10/762,330 Group Art Unit: 2132

Confirmation No. 4953

Filed: January 23, 2004 Examiner: Benjamin E. LANIER

For: SECURITY MANAGEMENT DEVICE AND SECURITY MANAGEMENT METHOD

DECLARATION UNDER 37 C.F.R. 1.131

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

I, Satoru TANAKA, declare that:

1. I am inventor of the above-identified US patent application, which claims foreign priority to Japanese Patent Application no. 2003-022630.

2. Prior to November 27, 2002, I conceived the idea of detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus, judging whether the security level of the user apparatus reaches a predetermined security level; and if the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network by the user apparatus, as described and claimed in the above-identified application. I also conceived the idea of determining a security level of a user terminal upon a network access for the user terminal, based upon one or more of security information updating history of the user apparatus, port access information of the user terminal, or programs and/or scripts downloaded and/or executable at the user terminal, and ensuring a predetermined security level on the network, according to the determined security level of the user terminal.

3. On or before November 27, 2002, I prepared an Invention Disclosure Record (IDR) (5 pages) including an Inventor Declaration (1 page) (copy attached hereto as Exhibit A) describing

my invention, which I forwarded to our in-house patent division member Mr. Akihito WAKAYAMA for the assignee Fujitsu Limited. The dates deleted from Exhibit A are prior to November 27, 2002.

4. The IDR (Exhibit A) shows the conception of at least claims 1, 5, 9 13, 15 and 27. The portions of the IDR evidencing conception are supplied as parenthetical annotations within copies of the claims set forth below, using claims 1, 13, 15 and 27 as examples. Claims 5 and 9 require substantially same limitations of claim 1 as respective method, recording medium and type claims.

1. A security management device including:

a security detection unit detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus (see Exhibit A pages 3, 4 and fig.2, 3);

a judging unit judging whether the security level of the user apparatus reaches a predetermined security level (see Exhibit A page 3, fig.2); and

an access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network by the user apparatus (see Exhibit A pages 4 and 5).

13. A security management system comprising:

a security management device, an apparatus for a user and a security setting guide device in communication via a network (see Exhibit A pages 4 and fig. 4),

wherein the security management device comprises:

a security detection unit detecting a security level of a user apparatus, based upon a record of updating a virus definition file of the user apparatus (see Exhibit A pages 3, 4 and fig.2, 3);

a judging unit judging whether the security level of the user apparatus reaches a predetermined security level (see Exhibit A page 3 and fig. 2); and

an access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network by the user apparatus (see Exhibit A pages 4 and 5).

15. A security management device including:

a controller

determining a security level of a user terminal upon a network access for the user terminal, based upon one or more of security information updating history of the user apparatus, port access information of the user terminal, or programs and/or scripts downloaded and/or executable at the user terminal (see Exhibit A pages 3, 4 and fig. 2), and

ensuring a predetermined security level on the network, according to the determined security level of the user terminal (see Exhibit A pages 4 and 5).

27. A method of managing security of a computer network to which a user terminal is communicably connected, comprising:

determining a security level of the user terminal upon access to the network from the user terminal, based upon security information updating history of the user apparatus, port access information of the user terminal, programs and/or scripts downloaded and/or executable at the user terminal, or any combinations thereof (see Exhibit A pages 3, 4 and fig. 2) and

ensuring a security level on the network, according to the determined security level of the user terminal (see Exhibit A pages 4 and 5).

5. On information and belief, on or about July 7, 2002, I sent a copy of the IDR (Exhibit A) to a patent search company as Fujitsu Techno Research Inc. via email requesting that a prior art search be conducted.

6. On information and belief, on or about July 29, 2002, Mr. Yoshifusa TOGAWA of the Fujitsu Techno Research, Inc. received the search report.

7. On information and belief, on or about July 29, 2002, the search report was forwarded to me (inventor) via email.

8. On or before September 12, 2002, I prepared comments concerning the prior art found in the search.

9. During the time period from September 12, 2002, namely the date I prepared comments concerning the prior art found in the search, and the date of my interview with a patent attorney at Shuwa Chizai, Inc., namely on or about November 20, 2002, our in-house patent division member sent an email message to patent attorneys employed at Shuwa Chizai Inc. sending the comments, and authorizing the preparation of a patent application the result of which was the preparation and filing of the Japanese priority application no. 2003-022630 for the above-identified US patent application, and requesting that an interview be scheduled with me (inventor) at the earliest convenience.

10. On or about November 20, 2002, we had an interview with a patent attorney employed at Shuwa Chizai Inc..

11. On information and belief, on or about December 30, 2002 the patent attorney employed at Shuwa Chizai Inc. provided me a draft of the patent application via email.

12. On or about January 16, 2003, I provided comments on the draft and on information and belief on that day the comments were forwarded by our in-house patent division member Mr. Hisao SUDA to the patent attorney employed at Shuwa Chizai Inc. via letter.

13. On information and belief, on or about January 21, 2003, Mr. Akihito WAKAYAMA instructed the patent attorney employed at Shuwa Chizai Inc. to file the Japanese priority application 2003-022630.

14. On January 30, 2003, the Japanese priority application 2003-022630 for the above-identified US patent application was filed in the Japan Patent Office.

15. All statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true, and furthermore these statement are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application of any patent issuing thereon.

Respectfully submitted,

Date: 2008/10/16 By: Satoru TANAKA

Satoru TANAKA

c/o FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome

Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588 Japan

Residence Address

EXHIBIT A

(A) 依頼元発信番号(identification No.) 8091 020143

発明者確認書 Inventor Declaration

私／我々は、添付に開示の発明を我々が年／月／日に着想／発明したことを宣誓する。

I/We declare that the invention disclosed in the attachment was conceived/made by me/us on

(B) [redacted] / [redacted] / [redacted] .

Year / Month / Date

(C) 発明者氏名 Inventor Name	(D) 署　名 Signature	(E) 署名日 Date	(F) 職制印 Stamp
Satoru Tanaka	田中 悟	[redacted]	[redacted]

証人確認書 Witness Declaration

私は、この書面に添付の説明書に記載の発明を確認し、理解したことを宣誓します。ここに私の理解の確認として確認日を記入し、署名及び押印致します。

I declare that I have reviewed and understood the invention disclosed in the attached paper. Here, I sign and put my stamp with the date as confirmation of my understanding.

(G) 確認者氏名 Witness Name	(G) 署　名 Signature	(I) 確認日 Date	(J) 職制印 Stamp
KAZUO IKEMOTO	池本 一夫	[redacted]	[redacted]

添付資料 Attachment: 原稿・図面 (K)

[全 6 頁 (含む本頁) Total 6 Pages(including this page)]

PATENT DESCRIPTION

Authored FPS) Development Department, First Division
Name Satoru Tanaka

1. Title of the Invention

Security router

2. Scope of Claims

(1) A method of detecting a security level of a terminal based on an access pattern of the terminal, thereby to change an access permission range.

(2) A method of guiding a terminal under access restriction to a given server, thereby to save a network administrator extra effort.

(3) A device that implements the above (1) and (2).

3. Detailed Description of the Invention

(1) Field of Industrial Application

The present invention relates to various types of portable information processing devices having a network connection function.

(2) Prior Art

· JP 2002-33756 A HUB with access limit function
No function for detecting a security level of a connected terminal is provided, and only preset access limit can be performed.

· JP 2001-256136 A (P2001-256136A) Network system
A method for automatic setting of security, which is applicable for sophisticating the automatic setting of the present invention.

· JP 08-316963 A Terminal security management device
The device performs centralized management of access rights on a user or terminal basis, which is not related to a security level of a terminal.

(3) Problems to be solved by the Invention

In a case where a terminal below a given security level is connected to a network, it is difficult to detect the terminal in question. In addition, even if the terminal in question is detected, in order to set the security level thereof to a required value, a network administrator is required to respond to each case.

(4) Means for solving the Problems

FIG. 1 illustrates a configuration diagram according to the present invention. Further, FIG. 2 illustrates a flow chart for requirement judgment.

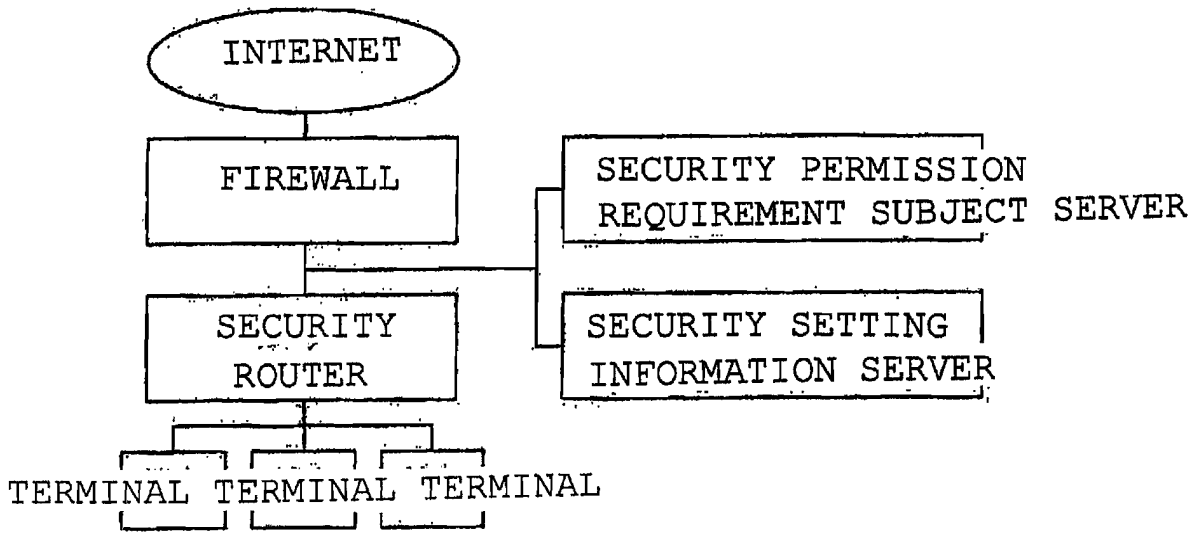

FIG. 1 CONFIGURATION DIAGRAM

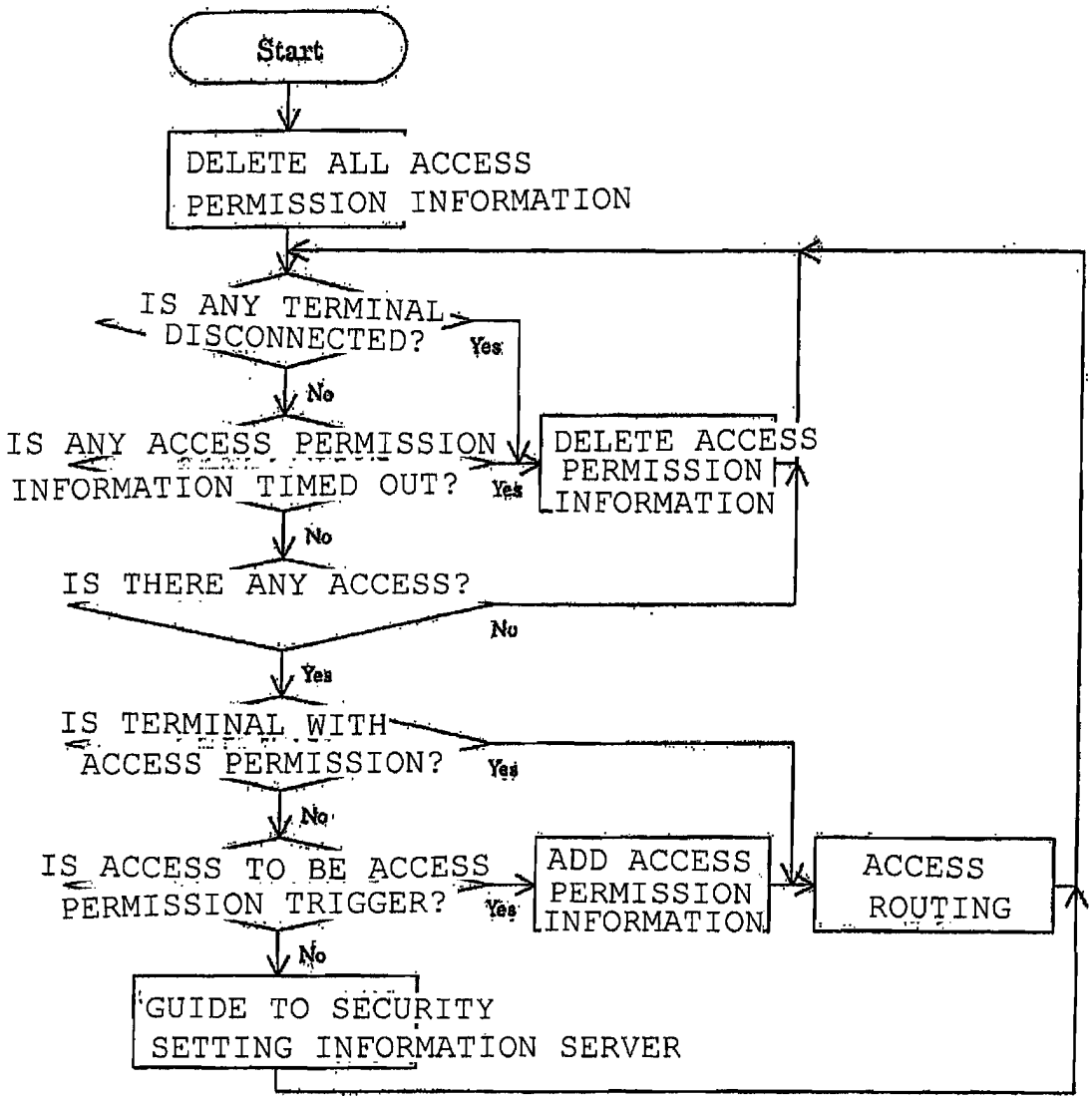

FIG. 2 FLOW CHART FOR REQUIREMENT JUDGMENT

(5) Action

When it is detected that a terminal has been connected to a router, unless a given operation (access to specified server or the like) is detected, a security level is judged to be below a required value, thereby allowing access to only a specific of servers.

Further, while the security level is below the required value, certain access is automatically guided to a security setting guidance server, and a user performs appropriate setting based on information thereof, thereby allowing the security level to be set to reach the required value. Accordingly, a network administrator can save extra effort.

(6) Embodiments

1) Embodiment of stand-alone type

A security router is prepared on a domain basis, and terminals are connected there below.

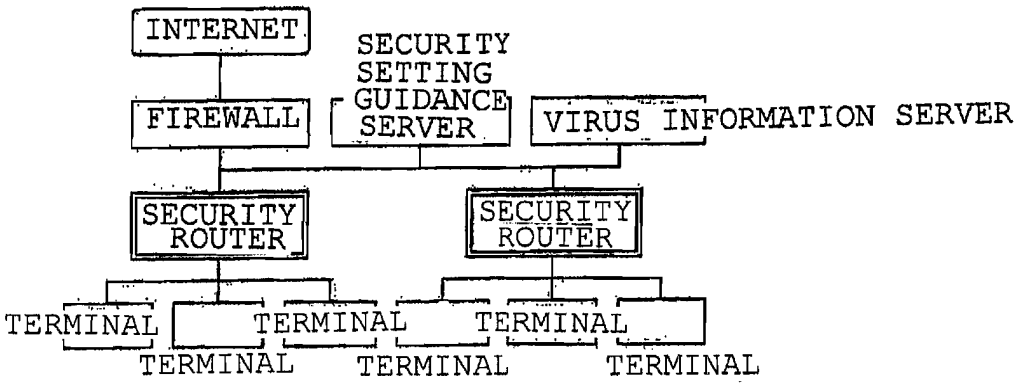

FIG. 3 IMAGE OF EMBODIMENT USING ROUTER

A requirement of a security level according to this example is access to a virus information server within a predetermined interval. Further, when the requirement of the security level is not satisfied, the security router allows only access to a security setting guidance server and the virus information server.

A characteristic is that the security router performs all of the monitoring/control.

2) Embodiment of built-in type to server or the like

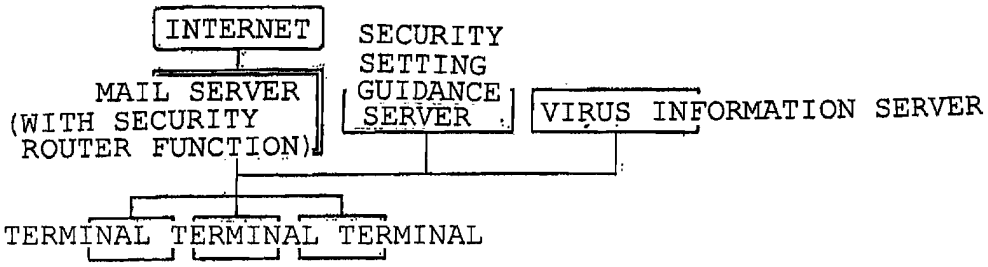

FIG. 4 IMAGE OF EMBODIMENT USING SERVER

According to this example, a mail server is used, but basically, the same applies to a proxy server/NFS/home gateway or the like.

A requirement of a security level according to this example is that, at the time of accessing a security subject server (mail server), a predetermined period of time has not yet elapsed since access to a virus information server.

A characteristic is that an access record is held by the virus information server and that a built-in routing program of the security subject server refers to information thereof to perform access control of the security subject server.

3) Advanced embodiment

According to the above 1)/2), the security level employs access to a given server as a reference, but instead, there is provided a method that employs a report from a security monitoring program.

For a predetermined period of time since the date and time when the monitoring program has confirmed that there is no problem, a security router allows access. It should be noted that, with regard to a monitoring record, there are provided a method of keeping the monitoring record in a terminal and a method of collecting the monitoring records in a given server.

(7) Effect of the Invention

Unless a terminal satisfies a requirement, a security router automatically guides access from the terminal in question to a security setting guidance server, and prohibits access to other domains or servers. Accordingly, an unauthorized access possible range is restricted, thereby ensuring security.

On the other hand, a user who does not satisfy the requirement is guided to the security setting guidance server by the security router, thereby enabling the user to acquire setting information for unrestricted use without any extra effort from an administrator. Accordingly, with regard to the terminal that can access other domains or servers, security of the terminal is inevitably kept above a required value.

As described above, for example, even if a terminal infected by a virus is connected, because of the insufficient security level, access is allowed to only a given range, thereby preventing spread of the infection. On the other hand, with regard to a terminal with a sufficient security level, anti-virus software is operating as prescribed to perform infection prevention/elimination of viruses, and hence, there is no fear of virus infection.